UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: **COMMISSIONER FOR PATENTS**
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,882	07/08/2003	Philip Michael Hawkes	030441	9835

			EXAMINER
23696	7590	02/15/2006	SIMITOSKI, MICHAEL J

QUALCOMM, INC
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 02/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/615,882	HAWKES ET AL.
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _30 November 2005_.

2a) ☒ This action is **FINAL.**   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-5,8-16,19-25,28-34,37-43,46-52 and 55-63_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-5,8-16,19-25,28-34,37-43,46-52 and 55-63_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _02 February 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   The response of 11/30/2005 was received and considered.

2.   Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 are pending.

Response to Arguments

3.   Applicant's arguments filed 11/30/2005 have been fully considered but they are not

persuasive.

As an initial note, claims 58-63 are indicated with the status identifier "new". However,

for the purposes of advancing prosecution, it is assumed that this status identifier is a

typographical error and that the correct identifier should be "previously presented" for those

claims. Applicant is reminded to provide updated status identifiers in accordance with 37 CFR

§1.121(c) with any further responses.

Applicant's response (p. 12) argues that "Lee does not teach or even suggest key

exchange". However, the phrase "key exchange" does not appear as a limitation in the claims.

Only distributing a key, which requires the data representing the key be moved or copied from

one location to another. The current claim language does not require a key to be transmitted over

a network.

Applicant's response (p. 12) argues that the random number does not function as a key,

but as a seed to reset the PN sequence generator. However, the claims recite no particular

algorithmic implementation of key transformations. In fact, the independent claims do not recite

using the secret key/random number in any way. As the random number seeds

(deterministically) the PN sequence generator, the seed is required in generating the correct

sequence, which is then required in decoding the signal; hence the random number acts as a key.

Applicant's response (pp. 12-14) makes the statement "if the public key is equated with the user ID, only for the purposes of argument, Lee does not teach or disclose distributing the user ID as claims 1, 22, 40 and 58." However, the Examiner respectfully disagrees. The user ID must be received by the user's station at some point. While it is suggested to be done "prior to installation" (Lee, col. 3, lines 65-67), even if this is done at manufacturing, the key is being distributed. Further, as modified by Menezes, Menezes teaches key layering where a master key is initially distributed (p. 551, §Master keys). Both the private key and public key must be distributed to their respective units for any encryption/decryption to take place. It is noted that Applicant has recited no features further limiting the limitation "distributing", such as a type of distributing, in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicant's response (p. 14) argues that Menezes does not teach an exchange of keys. However, while Menezes teaches transmitting the key (p. 553, ¶1), "exchange of keys" is not recited in the claims.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 & 55-63 are rejected under 35 U.S.C.

103(a) as being unpatentable over U.S. Patent Re. 33,189 to Lee et al. (**Lee**) in view of

Handbook of Applied Cryptography by Menezes et al. (**Menezes**).

Regarding claims 1, 22, 40 & 58, Lee discloses distributing a key/user ID (col. 3, lines

28-42), receiving a secret key encrypted by the key/user ID (col. 4, lines 1-22), decrypting the

secret key/ key by the key/user ID (col. 4, lines 1-22), receiving the access key/random number

encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random

number by the secret key/key (col. 4, lines 1-22). Lee lacks a public key. However, Menezes

teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-

encrypting keys are used to transport keys and data keys are used to encrypt the data a user will

use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to

encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig.

13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to use a public key to encrypt the secret key. One of ordinary skill

in the art would have been motivated to perform such a modification to achieve simplified key

management, as taught by Menezes (p. 551, #1-3).

Regarding claims 2, 10, 14, 20, 23, 29, 32, 38, 41, 47, 50, 56 & 59, Lee discloses the

secret key being a registration key (col. 2, lines 41-51).

Regarding claims 3, 11, 15, 21, 24, 30, 33, 39, 42, 48, 51 & 57, Lee discloses the secret

key being a temporary key/key of the month (col. 3, lines 28-42).

Regarding claims 4, 12 & 63, Lee discloses deriving a short key/PN sequence based on the access key/random number, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content using the short key/PN sequence (col. 3, line 28 - col. 4, line 22).

Regarding claims 5, 25, 43 & 60, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving the broadcast access key/key encrypted by the key/user ID and decrypting the broadcast access key/key by the private key/user ID (col. 4, lines 1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 8 & 61, Lee discloses deriving a short key/random number based on the access key/key, receiving encrypted broadcast content/video and decrypting the encrypted broadcast content/video using the short key/random number (col. 3, line 28 - col. 4, line 22).

Regarding claims 9, 28, 46 & 62, Lee discloses receiving a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), encrypting the secret key/key with the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 3, lines 1-22), receiving the access key/random number encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 3, line 28 - col. 4, line 22). Lee lacks

a public key. However, Menezes teaches that key layering is a key-exchange technique,

whereby a master key is distributed, key-encrypting keys are used to transport keys and data keys

are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches

that public keys can be used to encrypt other keys, which are then decrypted by the

corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to

one having ordinary skill in the art at the time the invention was made to use a public key to

encrypt the secret key. One of ordinary skill in the art would have been motivated to perform

such a modification to achieve simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 13, 31 & 49, Lee discloses receiving a key/user ID (col. 3, lines 28-42),

encrypting a secret key/key using the key/user ID (col. 3, lines 42-64), sending the encrypted

secret key/key (col. 4, lines 1-5), encrypting the access key/random number using the secret

key/key (col. 3, lines 42-64) and sending the encrypted access key/random number (col. 4, lines

1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange

technique, whereby a master key is distributed, key-encrypting keys are used to transport keys

and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically,

Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by

the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to use a public

key to encrypt the secret key. One of ordinary skill in the art would have been motivated to

perform such a modification to achieve simplified key management, as taught by Menezes (p.

551, #1-3).

Regarding claims 16, 34 & 52, Lee discloses receiving a key/user ID (col. 4, lines 1-22),

encrypting the broadcast access key/key using the key/user ID (col. 3, lines 42-64) and sending

the encrypted broadcast access key/key (col. 3, lines 42-64). Lee lacks a public key. However,

Menezes teaches that key layering is a key-exchange technique, whereby a master key is

distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt the

data a user will use (pp. 552-553, §13.3.1). Specifically, Menezes teaches that public keys can

be used to encrypt other keys, which are then decrypted by the corresponding private key (p.

552, #2 & Fig. 13.4(b)). Therefore, it would have been obvious to one having ordinary skill in

the art at the time the invention was made to use a public key to encrypt the secret key. One of

ordinary skill in the art would have been motivated to perform such a modification to achieve

simplified key management, as taught by Menezes (p. 551, #1-3).

Regarding claims 19, 37 & 55, Lee discloses distributing a key/user ID corresponding to

a private key/user ID (col. 3, lines 28-42), receiving a secret key/key (col. 3, lines 42-64)

encrypted by the key/user ID (col. 3, lines 42-64), decrypting the secret key/key by the private

key/user ID (col. 4, lines 1-22), encrypting the access key/random number by the secret key/key

(col. 3, lines 42-64) and sending the encrypted access key/random number (col. 3, line 28 - col.

4, line 22). Lee lacks a public key. However, Menezes teaches that key layering is a key-

exchange technique, whereby a master key is distributed, key-encrypting keys are used to

transport keys and data keys are used to encrypt the data a user will use (pp. 552-553, §13.3.1).

Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then

decrypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to use a

public key to encrypt the secret key. One of ordinary skill in the art would have been motivated

to perform such a modification to achieve simplified key management, as taught by Menezes (p.

551, #1-3).

Conclusion

6.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The

examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
    Commissioner for Patents

P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
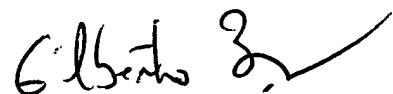(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
February 6, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100